REMARKS

Claims 1-30 are pending in this application. Claim 1 has been amended to put it into better form.

Rejection of the Claims under 35 U.S.C. § 112, Second Paragraph

Claims 1-30 were rejected under 35 U.S.C. § 112, second paragraph as failing to distinctly claim the present invention. Applicants respectfully request reconsideration of this rejection, the term "Bluetooth," though used as a trademark is definitive to meet the requirements of § 112, second paragraph. It refers to a wireless technology defined by a number of specifications well-known to those skilled in the art. Use of the term in patents is quite common. It is noted that a simple search of issued US patents brings up 387 examples of using the term "Bluetooth" in the claims. Indeed, claim 2 of the Struble reference cited in the present application uses the term, "Bluetooth technology" that is used in the present claim language. In view of the above, reconsideration and withdrawal of the rejection of claims 1-30 under 35 U.S.C. § 112, second paragraph is respectfully requested.

Rejection of the Claims under 35 U.S.C. §§ 102(e) and 103(a)

Claims 1-4, 7, 18-21, 24, and 29 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,647,497 to Cromer et al. ("Cromer"). Claims 5, 6, 8, 9, 22, and 23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Cromer in view of U.S. Patent No. 6,609,656 to Elledge ("Elledge"). Claims 10-17 and 25-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Cromer in view of Elledge in view of U.S. Patent No. 6,433,685 to Struble et al. ("Struble"). Claim 30 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Cromer in view of Struble.

The present invention concerns a Bluetooth security system where a secured device includes a communication system that allows it to communicate with a number of Bluetooth access points coupled to a security server. Claim 1, for example recites a plurality of Bluetooth Access Points that are to establish a Bluetooth link with the secured device and a security server that is connected to all BTAPs. Also, claim 1 calls for the security server to obtain attribute information, to activate a lock with the secured device, and to send location information of a

designated BTAP and an unlock code to the secured device via the designated BTAP. Claim 18 is a method claim that includes limitations similar to those found in claim 1. Claim 29 refers to a plurality of instructions stored on a computer readable medium to be executed by a processor of a security server to establish a link via a designated BTAP to obtain attribute information of the secured device, activate a lock with the secured device and sending location information of the designated BTAP and an unlock code to the secured device via the designated BTAP. Several features of these independent claims are not taught or suggested by the cited references.

Cromer concerns a method and apparatus for shipping a computer from a shipping point to a receiving point. The computer includes an RFID interface that is capable of receiving wireless signals (Col. 3, lines 44-47). The communication with the RFID interface occurs at the shipping point. Aside from the limitations of the claims concerning the Bluetooth specification, Cromer is silent as to the presence of a plurality of BTAPs as found in claims 1 and 18. The Office Action cites Col. 1, lines 37-40 and Col. 4, lines 28-33 as support for showing such a feature, but these sections merely refer to the RFID interface of the computer. Also, there is no disclosure in Cromer of sending location information of a designated BTAP and an unlock code via the designated BTAP as recited in all of the independent claims. Furthermore, there is no disclosure in Cromer of a security server connected to a designated BTAP to perform the functions recited in the independent claims. The Office Action simply states that the "shipping site" is a security server.

Elledge and Struble fail to make up for the deficiencies of Cromer. Elledge concerns the a plurality of receivers that receive information from RFID devices in an item such as a laptop computer. A computer with a database is able to verify whether the laptop computer has been detected by a receiver and that laptop has been stolen. In response to an appropriate match, an alarm is sounded at the receiver. Elledge does not mention at all a security server to transmit data to a secured device via a designated BTAP as found in the claims. Struble is similar to Elledge in that it provides a computer with a database that receives information from a detector of identification information and checks it against its database records. When a match is found, owner preference information associated with the identification is retrieved and transmitted. Thus, as with Elledge, Struble does not mention at all a security server to transmit data to a secured device via a designated BTAP as found in the claims.

In view of the above, reconsideration and withdrawal of the rejection of claims 1-30 under 35 U.S.C. §§ 102(e) and 103(a) is respectfully requested.

The Office is hereby authorized to charge any additional fees under 37 C.F.R. §1.16 or §1.17 or credit any overpayment to Deposit Account No. 11-0600.

Should the Examiner have any questions concerning this matter, he is invited to contact Applicants' undersigned attorney at 202/220-4255.

Respectfully submitted,

Date: 7/13/05

Shawn W. O'Dowd
Registration No. 34,687

KENYON & KENYON
1500 K Street, N.W., Suite 700
Washington, D.C. 20005-1257
Tel.: (202) 220-4200
Fax.: (202) 220-4201
DC1-575978